IN THE CLAIMS

Please AMEND the claims as follows:

1. (AMENDED) A method of determining a public key having [a] an optionally reduced length and a [factor p] number p, using GF(p) or $GF(p^2)$ arithmetic to achieve $GF(p^6)$ security, without explicitly constructing $GF(p^6)$, comprising the steps of:

2

selecting a number [q] q and a number [p] p such that $[p^{**2} - p + 1] \frac{p^2 - p + 1}{2}$ is an integer multiple of [q] q;

selecting a number [g] g of order [q] g, where [g] g and its conjugates can be represented by [B] g, where [Fg(x) = x**3 - Bx**2 + (B**p)x -1] g, where [g, g**(p-1), g**(-p)] g, g, g-1, g-2;

representing the powers of [g] g using their trace over the field $GF(p^2)$;

selecting a private key; and

computing a public key as a function of [g] g and the private key.

7. (AMENDED) A system for determining a public key having [a] an optionally reduced length and a [factor p] number p, using GF(p) or $GF(p^2)$ arithmetic to achieve $GF(p^6)$ security, without explicitly constructing $GF(p^6)$, comprising:

a processor for selecting a number [q] q and a number [p] p such that [p**2 - p + 1] p^2 - p + 1 is an integer multiple of [q] q;

said processor selecting a number [g] g of order [q] q, where [g] g and its conjugates can be represented by [B] \underline{B} , where [Fg(x) = x^{**3} - Bx^{**2} + (B**p)x -1] $\underline{F_g(X)} = X^3 - BX^2 + B^pX - 1$ and the roots are [g, $g^{**}(p-1)$, $g^{**}(-p)$] \underline{g} , $\underline{g}^{p/1}$, \underline{g}^{-p} ,

said processor representing the powers of [g] g and the private key using their trace over the field $GF(p^2)$;

said processor selecting a private key;

a memory coupled to said processor for storing the private key;

said processor computing a public key as a function of [g] g; and

a network interface for distributing said public key over a network.

13. (AMENDED) A computer program article of manufacture, comprising:

A31